

# Subtraction makes computing integers faster

Thatchaphol Saranurak\*      Gorav Jindal†

December 12, 2012

## Abstract

We show some facts regarding the question whether, for any number  $n$ , the length of the shortest Addition Multiplications Chain (AMC) computing  $n$  is polynomial in the length of the shortest division-free Straight Line Program (SLP) that computes  $n$ .

If the answer to this question is “yes”, then we can show a stronger upper bound for PosSLP, the important problem which essentially captures the notion of efficient computation over the reals. If the answer is “no”, then this would demonstrate how subtraction helps generating integers super-polynomially faster, given that addition and multiplication can be done in unit time.

In this paper, we show that, for almost all numbers, AMCs and SLPs need same asymptotic length for computation. However, for one specific form of numbers, SLPs are strictly more powerful than AMCs by at least one step of computation.

## 1 Introduction

### 1.1 Straight Line Programs and PosSLP

Consider a sequence of registers  $(a_0, a_1, \dots, a_l)$  where  $a_0 = 1$  and  $a_l = n$ . A division-free Straight Line Program (SLP)  $P$  is a sequence of *assignments*  $\{(*_i, j_i, k_i)\}_i$ . Each assignment  $(*_i, j_i, k_i)$  represents the operation  $a_i \leftarrow a_{j_i} *_i a_{k_i}$ , where  $*_i \in \{+, -, \times\}$  and  $0 \leq j_i, k_i < i$ .  $P$  can be viewed as an arithmetic circuit computing integer  $n$ , where 1 is the only given constant.

The number which  $P$  computes or the result of  $P$  is denoted by  $c(P) = n$ . The length of  $P$  is  $l$ , and is denoted by  $|P|$ . We denote the length of the shortest SLP computing a number  $n$  by  $\tau(n)$ .

The original motivation of this paper is this problem.

**Definition 1. PosSLP** is the following problem: Given a SLP  $P$ , does  $P$  compute a positive number ?

---

\*Universität des Saarlandes, thatchaphol.s@stud.uni-saarland.de

†Universität des Saarlandes, s9gojind@stud.uni-saarland.de

PosSLP was introduced by Allender et al. [1] to study the relationship between classical models of computation and computation over the reals in the Blum-Shub-Smale model [10].

In the Blum-Shub-Smale model, the inputs are elements of  $\bigcup_n \mathbb{R}^n \triangleq \mathbb{R}^\infty$ , and thus each machine accepts a “decision problem”  $L \subseteq \mathbb{R}^\infty$ . The machine can do all arithmetic operations and  $\leq$ -test over  $\mathbb{R}$  in unit time, and it has a finite set  $S$  of real *machine constants*. The set of decision problems accepted by polynomial-time machine over  $\mathbb{R}$  using only constants from  $S \cup \{0, 1\}$  is called  $P_{\mathbb{R}}^S$ . The union of the classes  $P_{\mathbb{R}}^S$  over all  $S$  is called *polynomial-time over  $\mathbb{R}$*  and is denoted  $P_{\mathbb{R}}$ . The subclass  $P_{\mathbb{R}}^\emptyset$  of “constant-free polynomial-time” is usually denoted by  $P_{\mathbb{R}}^0$ .

In order to relate computation over  $\mathbb{R}$  to the classical Boolean complexity classes such as P, NP, PSPACE, etc., we consider the *Boolean part* of decision problems over the reals  $L \subseteq \mathbb{R}^\infty$ , which is defined as  $BP(L) = L \cap \{0, 1\}^*$ . In other words, we consider only when the inputs are bit strings. The Boolean part of  $P_{\mathbb{R}}$  is naturally denoted by  $BP(P_{\mathbb{R}}) = \{BP(L) \mid L \in P_{\mathbb{R}}\}$ . The relationship between  $BP(P_{\mathbb{R}})$  and classical classes has been shown:

$$P/\text{poly} \subseteq BP(P_{\mathbb{R}}) \subseteq PSPACE/\text{poly}.$$

The lower bound is by Koiran [8] and the upper bound is by Cucker and Grigoriev [5]. In the “constant-free” case  $BP(P_{\mathbb{R}}^0)$ , it turns out that PosSLP precisely captures this class. In particular, Allender et al. [1] showed that

$$P^{\text{PosSLP}} = BP(P_{\mathbb{R}}^0).$$

This means that, given an oracle for PosSLP, one can efficiently simulate the constant-free<sup>1</sup> polynomial-time machines of the Blum-Shub-Smale model of real computation when the inputs are bit strings.

This shows interesting consequence because the well-known *Sum-of-square-roots* problem, which has many applications to computational geometry, is in  $BP(P_{\mathbb{R}}^0)$  [12]. In this problem, we are given positive integers  $d_1, \dots, d_n$  and  $k$ , and we want to decide whether  $\sum_{i=1}^n \sqrt{d_i} \leq k$ . The *Euclidean Traveling Salesman* problem, even though it has PTAS, is not known to be in NP because there is no known technique for exactly verifying the length of a given path without using Sum-of-square-roots as a procedure. This problem, hence, is in NP relative to the *Sum-of-square-roots* problem.

The above discussion suggests the non-trivial upper bounds for PosSLP is very interesting. The current best upper bound for PosSLP is between the 3<sup>rd</sup> and the 4<sup>th</sup> level of the counting hierarchy. In particular,  $\text{PosSLP} \in P^{\text{PP}^{\text{PP}^{\text{PP}}}}$  [1], which implies that the Sum-of-square-roots problem and the Euclidean Traveling Salesman Problem are also in the counting hierarchy.

There is yet another reason to be interested in PosSLP. In [1], it was also shown that the *generic task of numerical computation* (GTNC) is polynomial

---

<sup>1</sup>Actually, we have even that  $P^{\text{PosSLP}} = BP(P_{\mathbb{R}}^S)$  where  $S$  contains only real algebraic constants, as  $P_{\mathbb{R}}^S = P_{\mathbb{R}}^0$  [4].

time Turing equivalent to PosSLP. Thus, given the PosSLP oracle, we gain numerical stability for any algorithms.

## 1.2 Addition Multiplication Chains

An Addition Multiplication Chain (AMC), introduced in [2], is an SLP without subtraction. That is,  $*$   $\in \{+, \times\}$ . It can be viewed as a monotone arithmetic circuit computing integer. We denote the length of the shortest AMC computing a number  $n$  by  $\tau_+(n)$ .

Now, we ask whether for every number  $n \in \mathbb{N}$ ,  $\tau_+(n) \stackrel{?}{=} \tau(n)^{O(1)}$ : is the length of the shortest AMC computing  $n$  always polynomial in the length of the shortest SLP? If the answer to this question is “yes”, we can show that PosSLP is in the  $2^{nd}$  level of the polynomial hierarchy. Note that  $\text{PH} \subseteq \text{P}^{\text{PP}}$  by Toda’s theorem. So this is a much stronger upper bound.

*Claim 2.* If  $\tau_+(n) = \tau(n)^{O(1)}$ , then  $\text{PosSLP} \in \Sigma_2^{\text{P}}$ .

*Proof.* Given an SLP of size  $\tau(n)$ , we guess the AMC of size at most  $\tau(n)^{O(1)}$ , and then verify the equivalence of the given SLP and the guessed AMC.

If the SLP computes a positive number, we can guess a correct AMC, as  $\tau_+(n) = \tau(n)^{O(1)}$  by assumption. If not, then no such AMC exists because AMCs can compute only positive numbers.

To verify the equivalence, it is known that EquSLP, deciding if two SLPs compute the same number, is in  $\text{coRP}$ . So  $\text{PosSLP} \in \exists\text{coRP} \subseteq \exists\text{coNP} = \Sigma_2^{\text{P}}$ .  $\square$

On the other hand, it is also interesting to prove that the answer is “no”: to show that there exists some number  $n$  for which  $\tau_+(n) \notin \tau(n)^{O(1)}$ . This would demonstrate how subtraction helps generate integers super-polynomially faster, given that addition and multiplication can be done in unit time.

## 1.3 Our Results

In this paper, we show two facts regarding the question,  $\tau_+(n) \stackrel{?}{=} \tau(n)^{O(1)}$ .

- First, for almost all numbers  $n$ , SLPs and AMCs need the same asymptotic length for computing  $n$ .
- Second, for one specific form of numbers, SLPs are indeed strictly more powerful than AMCs by at least one step of computation. The hard instance we use to establish the lower bound for AMCs is  $2^{2^n} - 1$ , where  $n \in \mathbb{N}$ .

## 1.4 Polynomial Version of the Problem

The question  $\tau_+(n) \stackrel{?}{=} \tau(n)^{O(1)}$  can be rephrased as “do monotone arithmetic circuits computing *integer*  $n$  have significantly less power than usual ones?”.

In *polynomial* setting, where we are given variables  $x_1, \dots, x_n$  and any field constants and we want to compute some polynomial  $p(x_1, \dots, x_n)$ , this question

is well-studied. There are polynomials that required exponential size monotone arithmetic circuits, but can be computed by polynomial size usual arithmetic circuits.

For instance, Valiant [13] showed that such a hard instance is the perfect matching polynomial of the triangle grid graph. One fact used to establish the lower bound for monotone circuits is that every computed monomial can never be canceled. To show the upper bound for usual circuits, the fact that perfect matching polynomial is homogeneous is used; if we know that  $p(x_1, \dots, x_n)$  is a  $d$ -degree homogeneous component of another easy polynomial  $q(x_1, \dots, x_n)$  that can be computed in  $t$  steps, then  $p$  can be computed in  $O(d^3 + d^2t)$  steps.

In our integer setting, we have none of these nice properties. It seems that there is no integer counterpart for homogeneous polynomial. Moreover, each bit of the computed integers can always be canceled from one to zero. We refer the reader to a survey by Landau and Immerman [11] for an analogy between polynomial and integer problems.

## 2 Tight asymptotic bound for almost all numbers

In this section, we show that, for computing almost all numbers from  $2^n$  to  $2^{n+1}$ , both SLPs and AMCs of size  $\Theta(n/\log n)$  are sufficient and necessary. For the proof, we use ideas by Brauer [3] and Erdős [7], who showed similar results for addition chains. In [6], Moreira showed similar non-asymptotic bounds for SLPs.

**Lemma 3.** *For all numbers  $z \in [2^n, 2^{n+1})$ ,  $\tau(z), \tau_+(z) \in O(n/\log n)$ .*

*Proof.* Let  $z \in [2^n, 2^{n+1})$  be any  $(n+1)$ -bit number, and let  $k$  is an integer to be fixed later. We write  $n+1 = m \cdot k + r$  where  $0 \leq r < k$ .

The idea is to compute  $m$   $k$ -bit numbers  $u_i$ , and then concatenate them together to get  $z$ . We write

$$\begin{aligned} z &= u_0 + 2^r \sum_{j=1}^m u_j \cdot (2^k)^{j-1} \\ &= u_0 + 2^r (u_1 + 2^k (u_2 + 2^k (\dots (u_{m-1} + 2^k u_m) \dots))) \end{aligned}$$

Now we just compute all  $1, 2, 3, \dots, 2^k$ , taking  $2^k - 1$  assignments. From this, we have  $2^r, 2^k$  and  $u_i < 2^k$ , for all  $i$ . There are  $m$  additions and  $m$  multiplications in the expansion above.

Thus,  $\tau_+(z) \leq (2^k - 1) + 2m$ . Choose  $k = \lceil \log n - \log \log n \rceil$ . We get  $\tau_+(z) \in O(n/\log n)$ .

Since SLPs are just AMCs equipped with subtraction,  $\tau(z) \leq \tau_+(z)$ . Thus,  $\tau(z) \in O(n/\log n)$  as well.  $\square$

**Lemma 4.** *AMCs and SLPs of length  $n$  can represent at most  $2^{3n \log n}$  different numbers.*

*Proof.* We will prove the result for only SLPs, because the proof for AMCs is same.

We count the possibilities for each assignment. For the  $i^{\text{th}}$  assignment,  $a_i \leftarrow a_{j_i} *_{i} a_{k_i}$ , there are at most  $3 \times i^2$  choices, as there are 3 types of operation (2 types for AMCs) and  $j_i, k_i < i$ . Thus, there are at most  $\prod_{i=1}^n 3i^2 = 3^n (n!)^2 \leq 2^{n \log 3} \cdot 2^{2n \log n} \leq 2^{3n \log n}$  combinations, for SLPs of length  $n$ .  $\square$

**Theorem 5.** *For almost all numbers  $z \in [2^n, 2^{n+1})$ ,  $\tau(z), \tau_+(z) \in \Theta(n/\log n)$ , where “almost all” means the fraction of  $1 - 2^{-\epsilon n}$ , and  $0 < \epsilon < 1$ .*

*Proof.* We only prove this for SLPs again. Let  $d > 1$  be some constant. By Lemma 4, SLPs of size at most  $\frac{n}{3d \log n}$  can represent at most  $2^{n/d}$  different numbers.

Consider the numbers from  $2^n$  to  $2^{n+1} - 1$ . There are  $2^n$  numbers but only  $2^{n/d}$  of them can be computed by SLPs of size  $\frac{n}{3d \log n}$ . Let  $\epsilon = 1 - \frac{1}{d}$ . Thus, there are  $2^n - 2^{n/d} = 2^n(1 - 2^{-\epsilon n})$  numbers which need SLPs of size at least  $\frac{n}{3d \log n}$ . That is, almost all numbers in the range required SLPs of size  $\Omega(n/\log n)$ .

But Lemma 3 states that all numbers in this range can be computed by SLPs of size  $O(n/\log n)$ . This concludes the proof.  $\square$

Since any number  $z$  is in  $[2^n, 2^{n+1})$  for some  $n$ , we conclude that  $\tau_+(z) = \Theta(\tau(z))$  for almost all  $z$ .

### 3 Gap of One

In this section, we study the numbers of the form  $2^{2^n} - 1$ , where  $n \in \mathbb{N}$ . For convenience, let  $N = 2^{2^n}$ . We show that  $\tau(N-1) \leq n+2$ , but  $\tau_+(N-1) \geq n+3$ .

*Claim 6.*  $\tau(N-1) \leq n+2$

*Proof.* We first compute  $a_1 \leftarrow a_0 + a_0$ . So  $a_1 = 2$ . Then we square the current result  $n$  times to get  $a_{n+1} = 2^{2^n} = N$ . Finally,  $a_{n+2} \leftarrow a_{n+1} - a_0$ , as desired.  $\square$

We prove the lower bound for  $\tau_+(N-1)$  in 3 steps:

- There are more than 2 additions in any AMC computing  $N-1$ .
- There cannot be exactly 3 additions in any AMC computing  $N-1$ .
- There are less than 4 additions in any AMC of length at most  $n+2$  which computes  $N-1$ .

#### 3.1 More than 2 Additions

In this subsection, we show that there is no AMC computing  $N-1$  using only 2 or less additions.

When there are few additions in an AMC, we know some facts about the values of the registers  $(a_0, a_1, \dots, a_l)$  assigned in each step.

**Fact 7.** *The registers assigned in an AMC  $P$  between the  $k^{th}$  and  $k + 1^{th}$  additions have values of the form  $\prod_{i=1}^k \alpha_i^{e_i}$  where  $\alpha_i = \prod_{j < i} \alpha_j^{f_j} + \prod_{j < i} \alpha_j^{f'_j}$  and, for all  $j$ ,  $\min\{f_j, f'_j\} = 0$ . In particular,  $\alpha_1 = 2$ , and  $\alpha_2 = 2^c + 1$ , for some  $c \geq 0$ .*

*Proof.* We prove the statement by induction on  $k$ . For the base case, the numbers computed in  $P$  before the first addition can be only  $1 = \prod_{i=1}^0 \alpha_i^{e_i}$ .

For the inductive step, consider the  $k^{th}$  addition assignment  $a \leftarrow b + c$ , where  $b = \prod_{i=1}^{k-1} \alpha_i^{b_i}$  and  $c = \prod_{i=1}^{k-1} \alpha_i^{c_i}$ , by the induction hypothesis. Thus,  $a = \prod_{i=1}^{k-1} \alpha_i^{b_i} + \prod_{i=1}^{k-1} \alpha_i^{c_i}$ . We pull the shared factors out and get  $a = \prod_{i=1}^{k-1} \alpha_i^{\min(b_i, c_i)} \times \alpha_k$  where  $\alpha_k = \prod_{i=1}^{k-1} \alpha_i^{f_i} + \prod_{i=1}^{k-1} \alpha_i^{f'_i}$  and, for all  $i$ ,  $\min\{f_i, f'_i\} = 0$ . Since multiplications can not yield new factors into the sequence, all the numbers computed before the  $k + 1^{th}$  addition would be of the form  $\prod_{i=1}^k \alpha_i^{e_i}$ .

The first factor is  $\alpha_1 = 2$ , because the first addition is  $1 + 1$ . Since we just show that  $\alpha_2 = \alpha_1^{f_1} + \alpha_1^{f'_1}$  where  $\min\{f_1, f'_1\} = 0$ , as  $\alpha_1 = 2$ , it follows that  $\alpha_2 = 2^c + 1$ , for some  $c \geq 0$ .  $\square$

Next, we state two known properties of the number  $N - 1$  and Fermat number (cf. [9]).

**Fact 8.**  $N - 1 = F_n - 2 = \prod_{i=0}^{n-1} F_i$  where  $F_i = 2^{2^i} + 1$  is the  $i^{th}$  Fermat number.

**Fact 9.** *Fermat numbers are coprime to each other.*

**Lemma 10.** *In an AMC with  $k$  additions computing  $N - 1 = \prod_{i=1}^k \alpha_i^{e_i}$ , we have  $e_1 = 0$ , and  $e_2 \leq 1$ . Moreover, if  $e_2 = 1$ , then there is a unique index  $j$  such that  $F_j \mid \alpha_2$ .*

*Proof.* By Fact 7,  $\alpha_1 = 2$ . But  $N - 1$  is odd, so  $e_1 = 0$ .

As we know  $\alpha_2 = 2^c + 1$ , for some  $c$ , we now claim that there is a unique index  $j$ , such that  $F_j \mid \alpha_2$ .

There are 2 cases. If  $c$  is a power of 2,  $c = 2^j$ , then  $\alpha_2 = 2^{2^j} + 1 = F_j$ . Hence,  $j$  is a unique index such that  $F_j \mid \alpha_2$  by Fact 9.

Otherwise,  $c$  is not a power of 2,  $c = 2^j \cdot w$ , for some odd  $w$ , then  $\alpha_2 = (2^{2^j})^w + 1 = (-1)^w + 1 = 0 \pmod{F_j}$ . Thus,  $F_j \mid \alpha_2$ . For uniqueness, we show that for  $k \neq j$ ,  $F_k \nmid \alpha_2$ . If  $k < j$ , then  $\alpha_2 = (2^{2^k})^{2^{j-k} \cdot w} + 1 = (-1)^{2^{j-k} \cdot w} + 1 = 1 + 1 = 2 \pmod{F_k}$ . If  $k > j$ , then we write  $w = w' \cdot 2^{k-j} + w''$ , where  $w'' < 2^{k-j}$ . We have  $\alpha_2 = 2^{2^j w} + 1 = 2^{2^k w'} \cdot 2^{2^j w''} + 1 = (\pm 1) \cdot 2^{2^j w''} + 1 \pmod{F_k}$ . Since  $w'' < 2^{k-j}$ , so  $2^{2^j w''} + 1 < 2^{2^k} + 1 = F_k$ . So  $\alpha_2 = \pm 2^{2^j w''} + 1 \neq 0 \pmod{F_k}$ .

Now, we show that  $e_2 \leq 1$ . Since,  $F_j^{e_2} \mid \alpha_2^{e_2} \mid N - 1 = \prod_{i=0}^{n-1} F_i$ . If  $e_2 > 1$ , then  $F_j \mid \prod_{i \neq j} F_i$ . But this contradicts the coprimality of Fermat numbers, see Fact 9.  $\square$

**Theorem 11.** *If AMC computes  $N - 1$ , there are strictly more than 2 additions.*

*Proof.* If there is no addition, then the result is trivially 1.

If there is 1 addition, then the result can only be even number, but  $N - 1$  is odd.

If there are 2 additions,  $N - 1 = \alpha_1^{e_1} \alpha_2^{e_2}$ . By Lemma 10, it must be that  $N - 1 = \alpha_2$ , and there is only one  $j$ , where  $F_j \mid \alpha_2$ . So for  $k \neq j$ ,  $F_k \nmid N - 1$ , which contradicts Fact 8 :  $N - 1 = \prod_{i=0}^{n-1} F_i$ .  $\square$

### 3.2 Not 3 Additions

To prove the main statement in this subsection, we need this lemma.

**Lemma 12.** *Let  $S = \{2^{2^0}, 2^{2^1}, 2^{2^2}, \dots\}$  be the sequence of all numbers of the form  $2^{2^i}$ . Let  $A \subset \mathbb{Z} \setminus \{0, \pm 1\}$ ,  $B \subset \mathbb{Z}^+ \setminus \{1\}$  and  $C \subset \mathbb{Z}^+$  be finite sets.*

*For any increasing sequence  $T$  of the form  $\{c_i b_i^{e_i} + a_i\}_i$ , where  $e_i \in \mathbb{Z}^+$  and  $a_i, b_i, c_i \in A, B, C$  respectively, there are infinitely many indices  $i$  such that  $S_i \neq T_i$ .<sup>2</sup>*

*Proof.* Let  $\bar{a}, \bar{c}$  be the maximum elements in  $A$  and  $C$  respectively.

First, since  $A$  is finite and  $|a_i| > 1$ , so there exists a number  $t \in \mathbb{N}$  such that for all  $a_i$ ,  $a_i^{2^t} > \bar{a}$ . We fix such  $t$ .

Again, since  $A, B$  and  $C$  are finite and  $T$  is increasing, it follows that  $\{e_i\}_i$  is unbounded. So there exists  $i$  such that  $b_i^{e_i} > \bar{c}, \bar{a}^{2^{t \cdot |B|+1}}$ . Fix this  $i$ .

Consider the sequence  $\bar{B} = \{b_i, b_{i+t}, \dots, b_{i+t \cdot |B|}\}$ , there are  $b_j, b_{j'} \in \bar{B}$  such that  $b_j = b_{j'}$  where  $i \leq j < j'$ , because the size of  $\bar{B}$  is more than  $|B|$ . Note that  $t \leq j' - j \leq t \cdot |B|$ .

Now, we claim that for at least one index  $k \in \{i, j, j'\}$ , we have  $S_k \neq T_k$ . Suppose not, then we have  $c_k b_k^{e_k} + a_k = 2^{2^k}$  for all  $k \in \{i, j, j'\}$ . Thus, we get

$$(c_i b_i^{e_i} + a_i)^{2^{j-i}} = c_j b_j^{e_j} + a_j \quad (3.1)$$

$$\text{and } (c_j b_j^{e_j} + a_j)^{2^{j'-j}} = c_{j'} b_{j'}^{e_{j'}} + a_{j'} \quad (3.2)$$

We will show that  $b_{j'}^{e_{j'}} \geq b_j^{e_j} \geq b_i^{e_i}$ . To prove  $b_j^{e_j} \geq b_i^{e_i}$ , if  $i = j$ , then it is trivial. If  $i < j$ , suppose that  $b_j^{e_j} < b_i^{e_i}$ . This contradicts Equation (3.1), since

$$\begin{aligned} (c_i b_i^{e_i} + a_i)^{2^{j-i}} &\geq (c_i b_i^{e_i} + a_i)^2 \\ &= c_i^2 b_i^{2e_i} + 2a_i c_i b_i^{e_i} + a_i^2 \\ &> b_i^{2e_i} + b_i^{e_i} \\ &> c_j b_j^{e_j} + a_j \end{aligned}$$

The last inequality follows because  $b_i^{e_i} > b_j^{e_j}, \bar{c}, \bar{a}$ .

We can prove  $b_{j'}^{e_{j'}} \geq b_j^{e_j}$  in exactly same way using Equation (3.2). Now, since  $b_j = b_{j'}$ , we have  $e_{j'} \geq e_j$ . Consider Equation (3.2) modulo  $b_j^{e_j}$ . We have

---

<sup>2</sup> $a_i$  does not denote the  $i^{th}$  element of  $A$ , but it is just some element in  $A$  which constitutes the  $i^{th}$  element of  $T$ ,  $c_i b_i^{e_i} + a_i$ .  $b_i$  and  $c_i$  have similar meaning.

$$a_j^{2^{j'}-j} \equiv a_{j'} \pmod{b_j^{e_j}}$$

It follows that  $a_j^{2^{j'}-j} = a_{j'}$  because  $b_j^{e_j} \geq b_i^{e_i} > \bar{a}^{2^{t \cdot |B|+1}} > a_j^{2^{j'}-j}, a_{j'}$ . But  $t$  is such that  $a_j^{2^{j'}-j} \geq a_j^{2^t} > \bar{a} \geq a_{j'}$ , so we reach a contradiction. Thus, we have shown that for all  $i$  such that  $b_i^{e_i} > \bar{c}, \bar{a}^{2^{t \cdot |B|+1}}$ , we can find at least one index  $k \in \{i, j, j'\}$  where  $S_k \neq T_k$ , by considering the finite sequence  $\bar{B}$ . Now, since there are infinitely many  $i$  satisfying  $b_i^{e_i} > \bar{c}, \bar{a}^{2^{t \cdot |B|+1}}$ , we are done.  $\square$

**Lemma 13.** *If an AMC computes  $N-1$  using exactly 3 additions, then  $N-1 = 2^{d_1} \alpha_2^{d_2} + \alpha_2^{d'_2}$  where  $d_2 \leq 1$  or  $d'_2 \leq 1$ .*

*Proof.* By Lemma 10,  $N-1 = \alpha_2^{e_2} \alpha_3^{e_3}$  where  $e_2 \leq 1$ . We claim that  $e_3 = 1$ .

There is at most one  $j$  for which  $F_j \mid \alpha_2$ . So, for  $k \neq j$ , it must be that  $F_k \mid \alpha_3$ . We have  $F_k^{e_3} \mid \alpha_3^{e_3} \mid N-1 = \prod_{i=0}^{n-1} F_i$ . Now, if  $e_3 > 1$ , then  $F_k \mid \prod_{i \neq k} F_i$ , which contradicts the coprimality of Fermat numbers, see Fact 9.

We also have  $e_3 \neq 0$ , otherwise it must be that  $N-1 = \alpha_2$  which is impossible as shown in Theorem 11.

By Fact 7,  $\alpha_3 = \alpha_1^{f_1} \alpha_2^{f_2} + \alpha_1^{f'_1} \alpha_2^{f'_2}$ , where  $\min\{f_i, f'_i\} = 0$ . So  $N-1 = \alpha_2^{e_2} \alpha_3 = \alpha_1^{f_1} \alpha_2^{e_2+f_2} + \alpha_1^{f'_1} \alpha_2^{e_2+f'_2}$ . Since,  $\min\{e_2+f_2, e_2+f'_2\} \leq 1$ , we have the claim by rewriting the variables.  $\square$

**Theorem 14.** *There is no AMC computing  $N-1$  using exactly 3 additions.*

*Proof.* By Fact 7 and Lemma 13,  $N-1 = 2^{d_1} \alpha_2^{d_2} + \alpha_2^{d'_2}$  where  $\alpha_2 = 2^c + 1$ . We will show that, for any value of  $c, d_1, d_2$  and  $d'_2$ , an AMC with 3 additions cannot compute  $N-1$ .

First, neither  $c$  nor  $d_1$  can be zero. If  $d_1 = 0$ , then  $2^0 \alpha_2^{d_2} + \alpha_2^{d'_2}$  is even while  $N-1$  is odd. If  $c = 0$ , then  $N-1 = 2^{d_1+d_2} + 2^{d'_2} = 2^k + 1$  for some  $k$ , as  $N-1$  is odd. As in Lemma 10, if  $N-1$  is in this form, then there is only one index  $j$  such that  $F_j \mid N-1$ , and this contradicts the fact that  $N-1 = \prod_{i=0}^{n-1} F_i$ .

Now, there are 4 cases which all will lead to a contradiction : when  $c, d_1 \geq 2$ , when  $c \geq 3, d_1 = 1$ , when  $c = 1, d_1 \geq 3$ , and some remaining small cases, namely,  $(c, d_1) = (1, 1), (2, 1)$  or  $(1, 2)$ .

We use this following equality in the first two cases,

$$\alpha_2^d - 1 = (\alpha_2 - 1) \sum_{i=0}^{d-1} \alpha_2^i = 2^c \sum_{i=0}^{d-1} \alpha_2^i.$$

*Case 1.*  $c, d_1 \geq 2$ .

We have



$$\begin{aligned}
N - 1 &= 2^{d_1} \alpha_2^{d_2} + \alpha_2^{d'_2} \\
N &= 2^{d_1} \alpha_2^{d_2} + (\alpha_2^{d'_2} - 1) + 2 \\
N &= 2^{d_1} \alpha_2^{d_2} + 2^c \sum_{i=0}^{d'_2-1} \alpha_2 + 2.
\end{aligned}$$

Since,  $N = 2^{2^n}$  and  $c, d_1 \geq 2$ , the LHS is divisible by 4, but the RHS is not.

*Case 2.*  $c \geq 3$  and  $d_1 = 1$ .

We continue manipulating the equation from the last case, and set  $d_1 = 1$ .

$$\begin{aligned}
N &= 2\alpha_2^{d_2} + 2^c \sum_{i=0}^{d'_2-1} \alpha_2 + 2 \\
N/2 &= \alpha_2^{d_2} + 2^{c-1} \sum_{i=0}^{d'_2-1} \alpha_2 + 1 \\
N/2 &= (\alpha_2^{d_2} - 1) + 2^{c-1} \sum_{i=0}^{d'_2-1} \alpha_2 + 2 \\
N/2 &= 2^c \sum_{i=0}^{d_2-1} \alpha_2 + 2^{c-1} \sum_{i=0}^{d'_2-1} \alpha_2 + 2.
\end{aligned}$$

Since,  $c \geq 3$ , the LHS is divisible by 4, but the RHS is not.

*Case 3.*  $c = 1$  and  $d_1 \geq 3$ .

We have  $\alpha_2 = 3$ .

$$\begin{aligned}
N - 1 &= 2^{d_1} 3^{d_2} + 3^{d'_2} \\
N &= 2^{d_1} 3^{d_2} + (3^{d'_2} + 1).
\end{aligned}$$

One can check that, for any  $e$ ,  $3^e + 1$  is congruent to only 2 or 4 modulo 8. So the LHS is divisible by 8, but the RHS is not.

*Case 4.* The remaining cases.

This last case actually consists of many small cases. These are the cases when  $(c, d_1) = (1, 1), (2, 1)$  or  $(1, 2)$ , and we also have that  $d_2 \leq 1$  or  $d'_2 \leq 1$  by Lemma 13.

Fortunately, they can be handled simultaneously using Lemma 12. This lemma tells us that, if the computed numbers are of the form  $\{c_i b_i^{e_i} + a_i\}_i$ , where  $a_i, b_i, c_i$

are restricted to be from finite sets, and only  $e_i$  can be any number, then there are infinitely many  $n$ , where  $2^{2^n}$  does not occur in the sequence  $\{c_i b_i^{e_i} + a_i\}_i$ .

In this last case, we will show that  $2^{d_1} \alpha_2^{d_2} + \alpha_2^{d'_2} + 1$  is restricted to be of the form  $\{c_i b_i^{e_i} + a_i\}_i$  as in the lemma. So there are infinitely many  $n$ , where  $2^{2^n} = N \neq 2^{d_1} \alpha_2^{d_2} + \alpha_2^{d'_2} + 1$ , which would finish the proof.

To see this, observe that either  $d_2$  or  $d'_2$  is at most 1, hence only one of  $d_2$  or  $d'_2$  can be free variable. For example, when  $d'_2$  is not fixed and  $(c, d_1, d_2) = (1, 2, 1)$ , we have  $2^{d_1} \alpha_2^{d_2} + \alpha_2^{d'_2} + 1 = 3^{d'_2} + 13 = N$ . In this case,  $c_i = 1$ ,  $b_i = 3$ , and  $a_i = 13$ . After we list all possible cases, we have  $B = \{3, 5\}$ ,  $C = \{1, 2, 4\}$ ,  $A = \{2, 3, 4, 5, 6, 7, 11, 13\}$ , which are all finite sets and comply with the conditions of the lemma. □

### 3.3 Less than 4 Additions

In this subsection, we show that, if the length of an AMC  $P$  is at most  $n + 2$ , then  $P$  cannot compute the large number  $N - 1$  using 4 or more additions.

The main idea is that, to compute a large number using a short AMC, if there are too many additions, then there are not enough squaring steps. Indeed, to square the largest number is the fastest way to get a new big number. Hence, the final result cannot be as large as the desired number.

We show the following facts to argue this formally.

We say that two AMCs  $P = \{(*_i, j_i, k_i)\}_i$  and  $P' = \{(*'_i, j'_i, k'_i)\}_i$  are *equal (assignment-wise)* if  $(*_i, j_i, k_i) = (*'_i, j'_i, k'_i)$  for all  $i$ . We also say  $P$  is *transformed* into  $P'$  or  $P'$  is obtained from  $P$ , if  $P$  is manipulated such that it is equal to  $P'$ .

**Fact 15.** *Let  $P$  and  $P'$  be any AMCs with same numbers of additions and multiplications. We can transform  $P$  into  $P'$  by some sequence of these two operations:*

1. *Swapping the type of the operations of the  $i^{th}$  assignment with  $(i + 1)^{th}$  assignment. That is,  $*_i \leftarrow *_{i+1}$  and  $*_{i+1} \leftarrow *_i$ .*
2. *Incrementing/decrementing the index  $j_i$  or  $k_i$  of the  $i^{th}$  assignment. That is,  $j_i \leftarrow j_i \pm 1$  or  $k_i \leftarrow k_i \pm 1$ .*

**Definition 16. Irredundant AMC.** An AMC  $P$  is irredundant iff, for every  $i \in [0, |P| - 1]$ ,  $a_i < a_{i+1}$  and  $a_i$  is used as the operand in some assignment.

Here are easy facts about irredundant AMCs.

**Fact 17.** *If an AMC  $Q$  is redundant, then there exists an irredundant AMC  $P$ , where  $c(P) = c(Q)$  but  $|P| < |Q|$ .*

**Fact 18.** *For any irredundant AMC  $P$ , any increase (decrease) of the value of the register  $a_i$  of  $P$  always increases (decreases) the computed number  $c(P)$ .*

In the followings, we consider only irredundant AMCs because of this fact.

**Fact 19.** *If there is no irredundant AMC of size at most  $n + 2$  which computes  $N - 1$  using 4 or more additions, then neither is the redundant one.*

*Proof.* We prove the contra-positive. Suppose that  $Q$  is a redundant AMC of size at most  $n + 2$  which computes  $N - 1$  using 4 or more additions. Then there is an AMC  $P$ , where  $c(P) = c(Q) = N - 1$  but  $|P| < |Q| \leq n + 2$  by Fact 17. There are also at least 4 additions in  $P$ , otherwise this contradicts Theorem 11 or 14.  $\square$

**Fact 20.** *Let  $P$  be any irredundant AMC, and let  $\tilde{P}$  be obtained from  $P$  by incrementing some index  $j_i$  or  $k_i$ . We have  $c(P) < c(\tilde{P})$ .*

*Proof.* As  $P$  is irredundant,  $a_{j_i} < a_{j_i+1}$  and  $a_{k_i} < a_{k_i+1}$ . Hence,  $a_i$  would be increased. Then this fact follows immediately from Fact 18.  $\square$

We say that the AMC  $P$  has *maximum indices* if  $j_i = k_i = i - 1$ , for all  $i$ . That is, every register depends on only the previous one. Note that AMCs with maximum indices are irredundant.

**Fact 21.** *Let  $P$  be any AMC with maximum indices, and let  $\tilde{P}$  be obtained from  $P$  by swapping the operation  $*_i = \times$  with  $*_{i+1} = +$ . We have  $c(P) < c(\tilde{P})$ .*

*Proof.* For every  $i$ , let  $\tilde{a}_i$  be the  $i^{\text{th}}$  register of  $\tilde{P}$ . Since  $P$  and  $\tilde{P}$  have maximum indices, every register depends on only the previous one. It suffices to show that  $a_{i+1} < \tilde{a}_{i+1}$ .

We have  $a_{i+1} = 2a_i = 2a_{i-1}^2$  and  $\tilde{a}_{i+1} = \tilde{a}_i^2 = (2\tilde{a}_{i-1})^2 = (2a_{i-1})^2$ . Hence,  $a_{i+1} < \tilde{a}_{i+1}$  as desired.  $\square$

**Lemma 22.** *The maximum number that irredundant AMCs with  $a$  additions and  $m$  multiplications can compute is  $2^{a \cdot 2^m}$ .*

*Proof.* Consider an AMC  $P^*$  with maximum indices and the first  $a$  assignments are additions, followed by  $m$  multiplications. Actually, these additions are doubling and multiplications are squaring as  $P^*$  has maximum indices. Thus,  $c(P) = (2^a)^{2^m}$ .

We claim that, for any other irredundant AMC  $P$  with  $a$  additions and  $m$  multiplications,  $c(P) < c(P^*)$ . If  $P$  does not have maximum indices, then  $c(P) < c(P^*)$  by Fact 20. If  $P$  has maximum indices but  $P$  is not equal to  $P^*$ , then there exists an index  $i$  where  $(*_i, *_{i+1}) = (\times, +)$ . Hence,  $c(P) < c(P^*)$  by Fact 21. So  $P^*$  is the irredundant AMC with  $a$  additions and  $m$  multiplications which computes the biggest possible number.  $\square$

**Lemma 23.** *The second largest number that irredundant AMCs with  $a$  additions and  $m$  multiplications can compute is  $2^e$  where  $e = \max\{\log 3 \cdot (a - 2) \cdot 2^m, 3a \cdot 2^{m-2}, (2a - 1) \cdot 2^{m-1}\}$ .*

*Proof.* Consider  $P^*$  defined in the last lemma. We claim that, any irredundant AMC  $P$  computing the second largest number can be transformed into  $P^*$  in one manipulation.

Suppose that we need at least 2 manipulations to transform  $P$  into  $P^*$ . Since  $P^*$  has maximum indices, the manipulation contains no index decrement. Since two kinds of manipulation do not depend on each other, we assume that we always increment the indices and then swap the types of operations.

There are 2 cases. First, we need to increment index. After the first increment, we have  $\tilde{P}$  which is not  $P^*$  yet. We have  $c(P) < c(\tilde{P}) < c(P^*)$  by Fact 20 and Lemma 22. Second, we don't need to increment index, so  $P$  has maximum indices. After we swap the types of operations, we get  $\tilde{P}$  which is not  $P^*$  yet. We again have  $c(P) < c(\tilde{P}) < c(P^*)$  by Fact 21 and Lemma 22. In both cases,  $P$  computes at most the third largest number.

Now, having that we can get  $P^*$  from  $P$  in one manipulation, we can get  $P$  from  $P^*$  in one manipulation as well. There are many ways to manipulate  $P^*$  to get  $P$  in one step. But it turns out that there are only 3 possible values of  $c(P)$ .

First, we decrement one index of the addition assignment in  $P^*$ . So there is the assignment  $a_i \leftarrow a_{i-1} + a_{i-2}$  in  $P$ . The value of the register at the last addition is  $2^{a-i}(2^{i-1} + 2^{i-2}) = 2^{a-2} \cdot 3$ . Note that this does not depend on  $i$ . Then we square for  $m$  times, and get  $c(P) = (2^{a-2} \cdot 3)^{2^m} = 2^{\log 3 \cdot (a-2) \cdot 2^m}$ .

Second, we decrement one index of the multiplication assignment in  $P^*$ . Hence, there is the assignment  $a_{a+i} \leftarrow a_{a+i-1} \times a_{a+i-2}$  in  $P$ . Similarly, we have  $c(P) = (2^{a-2^{i-1}} \times 2^{a-2^{i-2}})^{2^{m-i}} = 2^{a \cdot 3 \cdot 2^{m-2}}$ .

Third, we swap the last addition with the first multiplication in  $P^*$ . We have  $c(P) = ((2^{a-1})^2 \cdot 2)^{2^{m-1}} = 2^{(2a-1) \cdot 2^{m-1}}$ .

The second largest number is the maximum among these results.  $\square$

Now, we are ready for the main statement.

**Theorem 24.** *If AMC computing  $N - 1$  has size at most  $n + 2$ , there are less than 4 additions.*

*Proof.* Let  $a$  be number of additions. If  $a \geq 5$ , then the biggest possible number is  $2^{a \cdot 2^m} \leq 2^{(n+2-a)+\log a} \leq 2^{2^{n-3}+\log 5} = 2^{2^{n-0.67}} < N - 1$ , for large enough  $n$ .

If  $a = 4$ , then the maximum number is  $2^{2^{(n+2-4)+\log 4}} = N > N - 1$ . Also, the second largest number is  $2^e$  where  $e = \max\{\log 3(4-2) \cdot 2^{n-2}, 3 \cdot 4 \cdot 2^{n-4}, (2 \cdot 4 - 1) \cdot 2^{n-3}\} = (2 \cdot 4 - 1) \cdot 2^{n-3} = 2^{n-3+\log 7}$ . We can see that  $2^{2^{n-3+\log 7}} < N - 1$ , for large enough  $n$ .  $\square$

We have shown that any AMC  $P$  computing  $N - 1$  must use strictly more than 3 additions by Theorem 11 and 14, but if  $P$  has size at most  $n + 2$ , then must be less than 4 additions as well. So  $\tau_+(N - 1) \geq n + 3$ . As  $\tau(N - 1) \leq n + 2$  by Claim 6, we conclude that subtraction helps us compute  $N - 1$  strictly faster by at least one step.

## 4 Conclusion

We have shown that, for almost all numbers  $n$ ,  $\tau_+(n) = \Theta(\tau(n))$ . We still suspect that there are hard instances  $n$  showing that SLPs compute some numbers super-polynomially faster than AMCs,  $\tau_+(n) \notin \tau(n)^{O(1)}$ . In this paper, we demonstrate the power of subtraction by showing only that  $\tau_+(N-1) - \tau(N-1) \geq 1$ , where  $N = 2^{2^n}$  and  $n \in \mathbb{N}$ .

However, note that  $N-1$  is not such hard instance because  $\tau_+(N-1) \leq 2n$ . This can be shown using the facts that  $N-1 = F_n - 2$  and, for all  $i$ ,  $F_i - 2 = F_{i-1} \times (F_{i-1} - 2)$ .

It remains as an open problem to decide whether there exists  $n$  such that  $\tau_+(n) \notin \tau(n)^{O(1)}$ . The next step towards this problem is to find  $n$  such that  $\tau_+(n) - \tau(n) = f(n)$  where  $f$  is some increasing function.

## Acknowledgments

We thank Markus Bläser for introducing us the problem and giving us useful comments and suggestions. Without his guidance, this work could not have been possible.

## References

- [1] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity, CCC '06*, pages 331–339, Washington, DC, USA, 2006. IEEE Computer Society.
- [2] Hatem M. Bahig. On a generalization of addition chains: Addition-multiplication chains. *Discrete Mathematics*, 308(4):611 – 616, 2008.
- [3] Alfred Brauer. On addition chains. *Bull. Amer. Math. Soc.*, 45(10):736–739, 1939.
- [4] Olivier Chapuis and Pascal Koiran. Saturation and stability in the theory of computation over the reals, 1997.
- [5] Felipe Cucker and Dima Grigoriev. On the power of real turing machines over binary inputs. *SIAM J. Comput.*, 26(1):243–254, February 1997.
- [6] Carlos Gustavo T. de A. Moreira. On asymptotic estimates for arithmetic cost functions. In *Proceedings of the American Mathematical Society*, volume 125, pages 347–353, 1997.
- [7] Paul Erdős. Remarks on number theory. iii: On addition chains (in english). *Acta Arith.*, 6:77–81, 1960.
- [8] Pascal Koiran. Computing over the reals with addition and order. *Theor. Comput. Sci.*, 133(1):35–47, 1994.

- [9] M. Krizek, F. Luca, and L. Somer. *17 Lectures on Fermat Numbers: From Number Theory to Geometry*. Springer, 2002.
- [10] M. Shub L. Blum, F. Cucker and S. Smale. *Complexity and Real Computation*. Springer, 1998.
- [11] Susan Landau and Neil Immerman. The similarities (and differences) between polynomials and integers. Technical report, 1994.
- [12] Prasoona Tiwari. A problem that is easier to solve on the unit-cost algebraic ram. *Journal of Complexity*, 8(4):393 – 397, 1992.
- [13] L. G. Valiant. Negation can be exponentially powerful. In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, STOC '79, pages 189–196, New York, NY, USA, 1979. ACM.